Employee-Owned Personal Devices

"BYOD" Policy

Page:	Last Revision Date:	Current Revision Date:	Policy/Notice Type:
1 of 8	07/21/2015	08/11/2015	Information Technology; Legal

This policy/notice may be updated from time to time. NOV will inform you of each update by either e-mail, the NOV intranet - http://inside.nov.com or through your local Human Resources representative.

1. PROGRAM OVERVIEW

The National Oilwell Varco group of companies, including your employer (collectively "**NOV**") have adopted an employee-owned personal devices (or "**EOD**") program to facilitate the use of employee-owned phones, tablets and similar electronic devices for NOV professional purposes ("**Program**").

Participation in the Program is strictly voluntary and is offered as a convenience to employees who prefer to use an EOD such as an iOS, Android, or Blackberry device or tablet to access NOV email and other information and to conduct NOV business, rather than using NOV-owned and issued devices. Participating employees are permitted to connect their EODs to the NOV network to conduct NOV business under the conditions described in this Policy. Participation in and availability of the Program may be subject to local legal requirements or restrictions in certain jurisdictions.

Participation in the Program is not a work requirement. Employees who prefer to use an NOV-owned and issued device and who are eligible for such a device based on their role and responsibilities may instead use a device owned and issued by NOV.

Access to the NOV network may be prohibited for EODs that are not protected through use of software installed as part of the Program. If you choose to participate in the Program, NOV may require installation of software on your registered EOD to create a segregated, encrypted working environment (the "**NOV Environment**") that provides access to NOV-related emails as well as communications, documents, information, content, applications, programs, data, databases, and other materials that may be available from the NOV network ("**NOV Information**").

2. YOUR PARTICIPATION IN THE PROGRAM AND ACCEPTANCE OF THIS POLICY

Prior to receiving approval to participate in the Program and connect your EOD to the NOV network, you must agree to comply with this Policy. By agreeing to this Policy, you acknowledge that you have read and understood this Policy and that you will fully comply with this Policy at all times. You understand that your failure to comply with this Policy at any time will at a minimum result in denial of access to the NOV network with your EOD and may lead to disciplinary action, including termination.

When deciding whether you are eligible to participate in the Program, NOV relies upon your acceptance of this Policy. If local law does not permit or recognize your agreement to this Policy, your request to participate in the Program will be denied.

3. ELIGIBLE EODS

Only devices and operating systems approved by NOV are permitted to access the NOV network. Typically any EOD that is able install the required software and can access the NOV network is

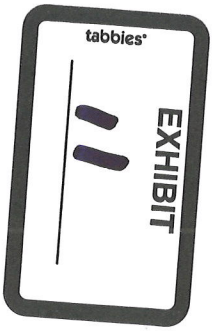

EXHIBIT
G

approved by NOV. NOV does not permit access to the NOV network or approve any EOD that has been modified to bypass security controls, such as a Jailbreak or Rooted devices.

4. REGISTRATION OF YOUR EOD

If you would like to participate in the Program, your request to participate will be granted only when NOV is satisfied that your participation meets all applicable requirements and therefore will not present undue risk or burden to NOV.

a. Registration of your EOD

You agree that in order to participate in the Program and access the NOV network you must first register your EOD with NOV.

b. Information collected from your EOD

You agree to allow NOV to collect device information, user identification, and other information for NOV's respective records. NOV may collect device and user information to be able to identify and locate an EOD, as well as to verify your compliance at all times with this Policy, and such information may be used as the basis for disciplinary action against you - up to and including termination for improper use/disclosure of NOV's proprietary or confidential information. Information that may be collected from you EOD includes:

- Device ID and name;
- Device manufacturer;
- Device type;
- Device OS version;
- User name and ID;
- UDID;
- IMSI;
- IMEI;
- IP address;
- Asset number;
- Phone number;
- Wifi / MAC address;
- RAM and storage;
- Display size;
- Power status;
- Physical memory;
- Number of apps;
- SIM card status;
- Country;
- Location;
- Status information;
- Corporate email;
- Texts (on certain OS);
- Program inventory; and/or
- Jailbroken/rooted information.

c. The Program Software

After registering an EOD and agreeing to follow the Policy, NOV may install or you may be required to download and install software (the "**Program Software**") on the EOD to establish certain security and other Program controls, including:

- device encryption;
- security settings;
- password or PIN requirements;
- digital certificates for authentication to the NOV Environment; and
- remote wipe capability to remove all content in the NOV Environment of the EOD.

5. SECURITY REQUIREMENTS FOR PARTICIPATION IN THE PROGRAM

a. EOD security requirements

To meet the NOV network's minimum security requirements you must verify that your EOD meets the following requirements:

- have up-to-date security patches;
- have password or PIN authentication for all accounts that can access the EOD;
- permit a maximum of 8 invalid attempts when logging into the EOD;
- contain up-to-date anti-virus and anti-spyware software;
- contain file or disk encryption;
- have up-to-date anti-malware software; and
- not have jailbreak or other security circumvention software, applications or tools (except for device unlock software provided by the telecommunications carrier for the device).

NOV can require the employee to present the device to confirm these minimum security requirements, at any time. From time to time NOV may publish additional settings and security requirements, such as password complexity requirements and lockout rules resulting from invalid login attempts. You agree that you are solely responsible for maintaining your own backups of information on your registered EOD other than Confidential Information (as defined below).

b. Managing EOD security settings

You agree to manage the security of your EOD by maintaining up-to-date software patches and anti-virus and malware updates from your telecommunications, hardware and software providers, and by implementing PIN, password and other protections in accordance with the specifications listed above.

You also agree that **NOV may access your device to manage the security settings of your EOD when you are accessing the NOV Environment, without providing further notice to you of such access or any changes to such security settings.**

6. EXPENSE REIMBURSEMENT

Certain employees may be eligible for a subsidy, reimbursement, or payment of certain services charges for EODs registered in the Program (e.g., phone and data charges), either at the company's sole discretion or as otherwise required by applicable local law.

7. CONFIDENTIAL AND PROPRIETARY INFORMATION

You acknowledge that your EOD may contain or provide access to proprietary or confidential information of NOV, its clients or other third parties ("**Confidential Information**"). You must protect

all Confidential Information on your EOD from unauthorized access or use and maintain the strict confidentiality of all Confidential Information.

You may not permit any other person to access the NOV Environment or any Confidential Information using your EOD, including family members and friends.

You must maintain logical segregation of all Confidential Information from your personal content or information in order to maintain confidentiality of all Confidential Information. Whenever possible you must ensure that no Confidential Information is stored or accessible on or through your EOD outside the NOV Environment.

Subject to any applicable law, NOV retains all ownership or other rights in or to all Confidential Information stored or accessible on any EOD and you acknowledge that you have no ownership or proprietary rights in or to any Confidential Information stored on or accessible via your EOD.

Without limiting its other rights, from the commencement of your participation in the Program NOV may access any Confidential Information stored on any registered EOD at any time with or without any further notice to you, subject to any legal restrictions or requirements.

8. USAGE OF EOD IN THE NOV ENVIRONMENT

a. Compliance with other NOV policies

Use of an EOD in the NOV Environment or otherwise in connection with any NOV-related work or activities is also subject to NOV's policies and guidelines, including without limitation:

i. the Code of Conduct;
ii. the Data Privacy and Protection Policy;
iii. the Use of the Internet, E-Mail and other Electronic Data Systems Policy; and
iv. the Employee Invention and Confidential Information Agreement.

You agree to comply with such policies and guidelines at all times.

b. Authorized and unauthorized use

Whenever possible, you may conduct NOV business using your registered EOD only in the secure NOV Environment. You may not use the personal section of your device -- such as using a Gmail account or other personal email account, or accessing social media sites such as Facebook and Twitter -- to conduct any NOV business or to access or use any Confidential Information.

You may not engage in any prohibited, unlawful, improper, offensive or otherwise inappropriate communications, conduct, activities or behavior using a registered EOD in the NOV Environment or otherwise in connection with any NOV-related work or activities.

Only NOV-approved applications and services may be installed or accessed within the NOV Environment.

You are solely responsible for backing up your personal information on your EOD and you are not permitted to back up any Confidential Information on your EOD.

9. REPORTING, MONITORING, AND OTHER PURPOSES

a. Reporting Security Breaches

"**Security Breach**" means any event that potentially or actually allows another individual access to any Confidential Information through an EOD. This includes, but is not limited to:

- temporary misplacement or permanent loss of the EOD;
- suspected or actual bypassing of access controls;
- suspected or actual misuse of the device and NOV accounts;
- suspected or actual infection of the device; or
- suspected or actual use of the device by another person.

You must immediately report any lost, stolen or damaged registered EOD or any Security Breach to the NOV IT Help Desk at (https://help.nov.com) or 1-888-44-NOVIT or check http://inside.nov.com for a list of additional help desk links and phone numbers for your respective work country.

b. Lost, stolen or damaged EOD

If possible, you must inform the NOV IT Help Desk at least 5 business days in advance if you plan to replace your registered EOD. If you wish to continue to participate in the Program, you will be required to register the new device and you authorize NOV to wipe any Confidential Information from the old device.

If your registered EOD is lost or stolen, NOV may remotely track its location solely to assist in attempting to recover the device.

c. Remote wipe of information on EOD

NOV may perform a remote wipe of any information, data, images, graphics, photos or content on any registered EOD that is lost, stolen or damaged, or when there is suspicion or threat of a Security Breach or other similar incident.

This may require wiping part or all of the memory or storage of a registered EOD, including personal or private content or information, if the Confidential Information cannot be easily or readily isolated for wiping. Wiping part or all of the device's memory or storage may result in irreversible damage to or erasure or destruction of any personal content or information stored on the EOD. NOV does not assume any liability for any damage, erasure or destruction of such content or information.

d. Investigations

You agree to cooperate with NOV as requested by NOV or its representatives or any legal, governmental, regulatory or quasi-regulatory authorities in the event of an investigation, examination, litigation, discovery request or other similar inquiry or process (an "**Investigation**"), including by preserving and providing access to the Confidential Information stored on your registered EOD for forensic or other analysis.

Subject to applicable law, in the event of an Investigation, including upon termination of your employment with NOV, NOV may retain your registered EOD and may obtain a copy of any Confidential Information on the device or engage an independent third party to make a copy (in which case no personal or private information shall be copied by or disclosed to NOV). Where a registered EOD is retained for the reasons above, NOV shall return the registered EOD within a reasonable period of time.

e. EOD monitoring

From the commencement of your participation in the Program, NOV will carry out ongoing, intermittent monitoring/surveillance of the use of your registered EOD in the NOV Environment, to the extent permissible by applicable law.

Such monitoring/surveillance is carried out by all means available to NOV which may include accessing information on your registered EOD, including your NOV email account or emails; accessing your NOV files (wherever stored) and other information contained in the NOV Environment on your registered EOD and using monitoring, logging and automatic alerting software and other specialized software.

Monitoring/surveillance will allow NOV to verify compliance with the minimum requirements for security and system settings as set forth in this Policy.

10. REPLACEMENT AND SUPPORT

Prior to taking your registered EOD to any service provider, vendor, technician or other person for support or changes, you must first notify the NOV IT Help Desk and follow any instructions they provide in order to protect Confidential Information stored on the device.

The NOV IT Help Desk will provide limited support for a registered EOD. Support may be limited to setup; support of NOV applications; installation of security and other software on your EOD; reporting theft, loss or replacement; and reporting of a potential or actual Security Beach. The NOV IT Help Desk may not provide general support for any EOD or assist with issues involving non-NOV applications.

11. DE-REGISTRATION, TERMINATION AND BREACH OF THIS POLICY

a. De-registration and termination

If at any time you would like to cease participating in the Program, you may de-register your EOD via the NOV IT Help Desk and all information, data, software, applications and other materials and content that belong to NOV, its customers or other third parties, and more generally all Confidential Information and Program Software, will be wiped from your EOD.

Upon any termination of your employment with NOV, you are expected to wipe from your EOD all information, data, software, applications and other materials and content that belongs to NOV, its customers or other third parties, and more generally all Confidential Information and Program Software. NOV retains the right, at its sole discretion, to wipe this content from your registered EOD by remote and/or direct means. You agree to present your EOD to the NOV IT Department in order to ensure and/or confirm that device has been wiped of NOV data and your access via the EOD to the NOV Environment has been revoked.

NOV may, at any time and without notice to you, terminate, suspend or block your registered EOD's access to the NOV Environment if, in NOV's sole and reasonable judgment, continued access may present an undue risk or burden to NOV (for example, if your registered EOD becomes outdated and a security risk, if certain services are no longer supported, in the event of user misconduct, failure to comply with this Policy, etc.).

NOV reserves the right to terminate the Program or your eligibility or participation at any time, including for non-use or inactivity of the Program Software.

b. Breach of this Policy

You agree to immediately notify the NOV Legal Department if you have breached or are unable or unwilling to comply with any or all of the terms and conditions of this Policy. Failure to comply with this Policy may result in disciplinary action, up to and including termination of employment.

In the event NOV has reason to believe that you may not be in compliance with all the requirements of this Policy, NOV may remove, limit, modify or suspend your participation in the Program. For example, actions that NOV might take could include:

i. Notify you, management and human resources of the issue and provide remediation instructions;
ii. Limit your registered EOD's access to certain applications and services;
iii. Block your registered EOD's access to all or part of the NOV Environment; and
iv. Bring your registered EOD into compliance by forcing software, packages or settings to be installed on the EOD, which could result in loss or corruption of your personal data or information stored on the device.

12. POLICY STATUS, CHANGES, AND UPDATES

This Policy does not form part of any employment contract with NOV. NOV may modify this Policy at any time and will inform you of any material change by providing you with access to the new Policy. Your continued use of your EOD after notification of the change will constitute your acceptance of the change. NOV may at any time revoke this Policy and discontinue permitting employees to use EODs to access the NOV Environment and NOV data.

13. SHARING YOUR PERSONAL DATA

Your NOV employer may share your collected EOD information with the following recipients:

- NOV information technology,
- NOV compliance,
- NOV human resources,
- NOV legal department,
- third-party software vendor in connection with administering the software, and/or
- the information will not be shared with anyone else outside of NOV unless required for law enforcement, legal proceedings, or otherwise required by applicable law

for the purposes set forth in this Policy. Recipients may be located other than in the country where you work. These disclosures will be made in compliance with applicable data privacy laws. For example, disclosure may be made to US entities that have certified adherence to the EU-US Safe Harbor Principles or to entities that have signed standard contractual clauses approved by the European Commission, in order to ensure protection of your personal data.

14. YOUR RIGHT TO ACCESS, CORRECT, DELETE AND OBJECT TO THE PROCESSING

You may have the right to access and correct personal data concerning you, subject to limited exceptions that may be prescribed by local law. Where justified and allowed by applicable law, you may also require that data be deleted or object to further processing of your data.

Your rights of access, correction, deletion, cancellation and objection are exercised by contacting the NOV IT Help Desk or your local human resources representative.

I ACKNOWLEDGE AND AGREE THAT I HAVE READ AND UNDERSTOOD THIS POLICY AND AGREE TO COMPLY WITH THIS POLICY AT ALL TIMES. TO THE EXTENT REQUIRED BY LAW, I EXPRESSLY

I ACKNOWLEDGE AND AGREE THAT I HAVE READ AND UNDERSTOOD THIS POLICY AND AGREE TO COMPLY WITH THIS POLICY AT ALL TIMES. TO THE EXTENT REQUIRED BY LAW, I EXPRESSLY AUTHORIZE ALL ACTIONS (INCLUDING WIPING OF INFORMATION ON MY REGISTERED EOD AND TRACKING THE LOCATION OF MY REGISTERED EOD) AS DESCRIBED IN THIS POLICY.

Employee's Printed Name	Julio C. Gomez
Employee's HCM Number	4023623
Employee's Signature	
Date	5-13-19

Print, sign and provide to your local HR representative upon signature.